AR-06-073

Office of Inspector General

Independent Evaluation Report

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2006

September 30, 2006

EXECUTIVE SUMMARY

Introduction

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. The FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

FISMA defines information security as "… protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (i) integrity—guarding against improper information modification or destruction and ensuring information nonrepudiation and authenticity; (ii) confidentiality—preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (iii) availability—ensuring timely and reliable access to and use of information."

The OIG found that FTC's Office of Information and Technology Management (ITM) continues to make progress in developing a mature information security program and has implemented or addressed OIG identified security vulnerabilities discussed in previous independent evaluation reports and other security reviews.

The OIG also conducted an internal scan of the FTC network environment on September 7 and 8, 2006. The results of the scan will be reported to the agency under a separate document.

Notwithstanding the progress made by the FTC, the OIG identified weaknesses and vulnerabilities that merit management's attention. The more important findings are listed below.

- FTC's Disaster Recovery Plan needs further development. The identified alternate sites at 601 New Jersey Avenue and the East Central Regional Office (ECRO) do not have sufficient space, power, or HVAC capability to function as a backup site for the FTC, if the main data centers were disabled. Additionally, there was no evidence that memoranda of understanding (MOU), service level agreements (SLA), or agreements with the General Services Agency (GSA) are in place to provide the extra resources needed at ECRO.

- FTC has contracted with ICF Consulting (ICF) for the use of Commentworks[SM] software to receive and process comments from the public on proposed regulatory

action. The FISMA review found that FTC managers responsible for CommentWorks[SM] are not notified when FTC employees leave the organization or are transferred within the organization and no longer need access to the system. Additionally, the review discovered that there is no contingency plan for ICF or CommentWorks[SM].

- Policies, procedures, and related security documentation for the Internet Lab either do not exist or are not documented. There are no documented policies, procedures, or forms for requesting, approving, or creating/removing user accounts for the Internet Lab. OIG was also advised that user IDs and passwords are not required for users to log onto and access Internet Lab workstations. There are no documented maintenance procedures. Backups are not conducted at this time; however, raw data is archived.

- The East Central Regional Office may take longer to recover from an incident since they do not have a contingency plan. All regional offices rely on Headquarters for contingency planning and disaster recovery. The FTC DRP and Continuity of Government kit do not address recovery of regional offices.

ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
APA	Administrations Procedure Act
BCP	Bureau of Consumer Protection
BIA	Business Impact Analysis
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIS	Consumer Information System
CPU	Central Processing Unit
DOJ	Department of Justice
DPI	Division of Planning and Information
DRP	Disaster Recovery Plan
ECRO	East Central Regional Office
FFS	Federal Financial System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
FY	Fiscal Year
GISRA	Government Information Security Reform Act
GSS	General Support System
HSPD	Homeland Security Directive
HVAC	Heating, ventilation, and air conditioning
IG	Inspector General
IP	Internet Protocol
ISA	Interagency Service Agreement
IT	Information Technology
ITM	Information and Technology Management
MMS	Matters Management System
MOU	Memoranda of Understanding
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBX	Private Automatic Branch Exchange
POA&M	Plan of Action and Milestones
PSTN	Public Switch Telephone Network
RAID	Redundant Arrays of Independent Disks
SLA	Service Level Agreement
SP	Special Publication
SSN	Social Security Number
ST&E	Security Testing and Evaluation
UPS	Uninterruptible Power Supply
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network

TABLE OF CONTENTS

1 Background

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, and outlined information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA included new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

2 Objectives

The objectives of the independent evaluation of the FTC information security program were to:

1. Assess compliance with FISMA and related information security policies, procedures, standards, and guidelines.

2. Determine the effectiveness of information security policies, procedures, and practices as implemented at Headquarters and the East Central Regional Office (ECRO) in Cleveland, Ohio.

3. Perform a network scan of the FTC Infrastructure network to identify vulnerabilities in the agency's security controls and patch management program.

4. Assess FTC's government equipment usage process.

5. Assess FTC's disaster recovery and contingency planning capability.

6. Evaluate security controls protecting FTC applications.

3 Scope and Methodology

The scope of this independent evaluation of the FTC fiscal year (FY) 2006 information security program included:

1. Review of two FTC major applications and related security documentation:
    a. CommentWorks[SM]
    b. Internet Lab

2. POA&M review for completeness and accuracy

3. Self-assessment review
4. Access to share drives
5. Voice Over Internet Protocol (VOIP) security
6. Government equipment usage
7. Remote access security
8. Contingency planning and disaster recovery
9. Scan of the FTC network
10. Regional Office visit to the ECRO in Cleveland, Ohio

To accomplish the review objectives, the OIG conducted interviews with Information and Technology Management (ITM) staff including the Chief Information Officer (CIO), the Senior Information Security Officer, other members of the ITM staff and ECRO personnel. The team reviewed documentation provided by the FTC including security plans, risk assessments, the disaster recovery plan (DRP), certification and accreditation (C&A) packages, privacy impact assessments, information security budgets, and other security related policies. The OIG also reviewed the security controls associated with FTC's VOIP telephone system, remote access controls, share drive access, and government equipment usage. Additionally, the OIG performed a scan of the FTC's information technology (IT) network and applications. The OIG also visited the ECRO to evaluate logical access controls, hardware inventory, and the continuity of operations/disaster recovery/physical security controls at the office to determine their effectiveness. Finally, the review included site surveys, documentation reviews, and interviews with FTC personnel.

All analyses were performed in accordance with guidance from the following:

1. Office of Management and Budget (OMB) Memorandum M-05-15, *Reporting Instructions for the Federal Information Security Management Act*, June 13, 2005
2. OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 17, 2006
3. FTC policies and procedures
4. *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Syste*ms, December 1998
5. Small Agency Council Memorandum SACCIO-05-1
6. *NIST SP 800-26, Self-Assessment Guide for Information Technology Systems*, August 2001

7. *NIST SP 800-30, Risk Management Guide for Information Technology Systems*, July 2004

8. *NIST SP 800-34, Contingency Planning Guide for Information Technology Systems*, June 2002

9. *NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004

10. *Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems*, February 2004

11. Quality Standards for Inspection issued by the President's Council on Integrity and Efficiency

12. GAO, *Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits*, January 1999

13. FTC/OIG audit guidance

14. OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002*

15. OMB Guidance M-04-15, *Guidance for Development of Homeland Security Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Infrastructure and Key Resources*

Fieldwork was conducted between May 25 and August 15, 2005.

4 General Overview

ITM continued to progress in developing a mature information security program and has implemented or addressed many of the OIG-identified security vulnerabilities discussed in FY 2005 independent evaluation report and in other security reviews and vulnerability scans. For example the FTC:

1. Updated ITM policies

2. Updated procedures for the Federal Financial System (FFS)

3. Finalized an Interagency Service Agreement (ISA) between FTC and the Department of Justice (DOJ) for e-Premerger

4. Certified and accredited CommentWorks[SM]

5. Conducted risk assessments, security plans, and security control reviews for an Internet Lab and the Litigation Support Lab

6. Added 64 new weaknesses to the POA&M from a variety of IT security reviews; while, successfully taking corrective action on 45 existing weaknesses

7. Made additional progress in developing an effective disaster recovery plan by developing a Continuity of Government kit that contains all the software and documentation ITM needs to reconstruct IT operations

8. Took steps to secure FTC's Private Automatic Branch Exchange (PBX) VOIP system

9. Implemented controls that restrict access to FTC's share drives

FTC is also in the process of developing and implementing policies and procedures to secure FTC's data stored on portable devices and media. At the FTC's ECRO, the OIG observed physical and operational controls in place to safeguard data. All staff interviewed attended the FTC security awareness training, and our interviews revealed that staff is aware of and follow FTC policies and procedures.

Notwithstanding the controls in place at FTC Headquarters and the ECRO, the OIG found other areas where improvements are still needed.

5 E-Gov Systems Update at FTC

In the FY 2005 Independent Evaluation, OIG reported:

> Based upon discussion with ITM personnel and the OIG's review of Memorandum M-03-22, OMB Guidance for Implementation of the Privacy Provisions of the E-Government Act of 2003, September 26, 2003, the FTC has no E-Gov systems (OIG Report AR 05-068 at p. 7).

Accordingly, OIG did not report that the FTC was required under the E-Government Act to conduct reviews and report to OMB on how information that is collected through information technology is handled to assure that personal information is protected.

During this year's review, OIG learned that there was a misunderstanding as to the scope of OIG's inquiry. OIG and ITM now agree that there are FTC information systems that fall within the definition of E-GOV. Such systems include, but may not be limited to, the Do Not Call Registry, the Electronic Consumer Complaint System, Consumer Sentinel, and Electronic Pre-merger Filing. OIG also understands that the agency has submitted reports to OMB regarding its compliance with the privacy provisions of E-Government Act.

OIG intends to work with management to fully resolve the issue of the applicability of the E-Government Act to the agency's collection and sharing of information gathered through information technology and to address the issue of the adequacy of the agency's privacy compliance in next year's report.

6 East Central Regional Office (ECRO) Review

As part of the FISMA review OIG visited the East Central Regional Office in Cleveland, Ohio, to evaluate the controls implemented in the following areas of system access control, hardware inventory, physical security, and contingency planning. Techniques used to conduct the review included site surveys, visual verification, and interviews. The results of the review are discussed below.

6.1 Access Control

Access Control is defined as the process of limiting access to the resources of an IT system only to authorized users, programs, processes, or other IT systems. A system's confidentiality, integrity, and availability are preserved by controlling access to information systems and associated networks. The ECRO's network access control was evaluated by comparing a list of the ECRO access control list provided by ITM with an FTC ECRO roster. Comparison of the lists confirmed that the access control list (ACL) contained all active ECRO staff members, plus two FTC employees who are not ECRO members, but are involved in investigations being conducted by the office. The name of one former intern was still on the ACL, but the account was identified as disabled. OIG confirmed that accounts of personnel leaving the agency are disabled in a timely manner.

Recommendation

None

6.2 Hardware Inventory Management

OIG evaluated the accuracy of the hardware inventory at the ECRO. This review was conducted by comparing the inventory list provided by ITM with the hardware located at the office. The findings are discussed below.

Finding # 1: East Central Regional Office does not have a reliable inventory of its IT equipment.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) requires that organizations develop, document, and maintain a current baseline configuration of the information system and an inventory of the system's constituent components.
Barcodes and, when possible, serial numbers were checked to see if they matched the inventory sheet provided by ITM. The review found a number of anomalies. These anomalies are listed below:

1. Not all equipment had barcodes. This equipment included two servers and the ROLM phone system. In addition, a Hewlett-Packard LaserJet IIIsi printer did not have a barcode.

2. Not all equipment is included on the official inventory. This equipment consisted primarily of monitors.

There are several possible reasons for this. One reason is that new monitors were shipped to the Cleveland office, and the master inventory list was not updated at the time the inventory list was created. The reason some equipment did not have barcodes may have been because the equipment was old and may not have been bar-coded and entered into the inventory.

The effect of not having an accurate inventory is that the agency may not have a complete assessment of available equipment. Additionally, not having an accurate inventory makes it difficult to identify missing or destroyed hardware.

Recommendation

ITM needs to update the East Central Regional Office's inventory.

ITM Response

ITM accepts the finding and has started an inventory of all Regional Office hardware with an expected completion date of 9/25.

OIG Response

We concur with ITM and will consider the finding closed upon verification during the POA&M review**.**

6.3 Physical Computer Environment

The East Central Regional Office of the FTC is located in suite 200 of the Eaton Center located at 1111 Superior Avenue, Cleveland, Ohio. The suite contains office space, file rooms, a hearing room, and an IT server room. OIG conducted site surveys and interviews to evaluate the physical security controls implemented at the ECRO.

Finding #2: ECRO computer room needs improved environmental controls.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) states that for specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization should provide the capability of shutting off power to any IT component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

Additionally, SP 800-53 requires that organizations monitor and maintain acceptable temperature and humidity levels within areas containing information systems.

The site survey conducted at the facility found a number of safeguards in place that protect FTC personnel and IT assets. These safeguards include:

Eaton Center Building:

1. A guard desk is located in the lobby and a magnetic card key is required to use the elevators.
2. Access to the building is restricted 24x7. Cardkeys for the building and elevator are needed.
3. Fire drills are conducted annually.
4. Fire extinguishers are inspected annually.
5. Fire safety inspections are conducted regularly and when a suite is renovated for a new tenant. If renovations are extensive, the floors immediately above and below the renovated floor/suite are also inspected.
6. Smoke detectors, fire extinguishers, and manual fire alarms are located throughout the building.
7. There is emergency battery lighting and a generator to maintain elevators, lighting, and sump pumps.
8. Video surveillance cameras are located throughout the interior and exterior of the building. Guards monitor the cameras 24x7.

Suite/Floor:

1. The suite is located on the second floor of the building. Windows are permanently sealed. There is a ledge where cooling equipment is located. This area is covered by metal grating, and the entrance to the area below the grating is reportedly locked. That this area is locked could not be verified.
2. Exterior walls of the suite have true floor to ceiling walls.
3. Suite doors are locked and alarmed at all times. Access to the suite requires a pass code. An additional pass code for the alarm system is required for after hours access. There is a guard desk in the lobby and a magnetic card key is required to use the elevators.
4. Exterior doors are alarmed and require key pad access. Some doors also have a magnetic lock.

Server (Computer) Room:

1. The server room is protected by the controls in place that protect the building and suite.
2. There are no windows in the computer room.

Two weaknesses relevant to the security of the office's IT equipment were also identified.

1. Server room has insufficient HVAC capability and, therefore, the server room door must remain open at all times.
2. There is no emergency power shut-off switch in the computer room.

Recommendations

1. Install a master power shutoff switch in the computer room
2. Improve HVAC capability of the computer room.

ITM Response

ITM accepts the finding and will work with ASO to evaluate the feasibility of making the recommended changes.

OIG Response

OIG concurs with ITM and will close this finding upon notification from ASO.

6.4 FTC/East Central Regional Office (ECRO) Contingency Planning and Disaster Recovery

OIG evaluated the ECRO to determine if there is a contingency plan for the office. The evaluation was conducted using site surveys, interviews, and documentation reviews.

Finding # 3: The ECRO does not have its own contingency or disaster recovery plan.

NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, dated February 2006, requires the use of NIST SP 800-53 security controls. Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain: (i) the security control title; (ii) how the security control is being implemented or is planned to be implemented; (iii) any scoping guidance that has been applied and what type of consideration; and (iv) whether the security control is a common control and who is responsible for its implementation.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated July 2002, differentiates security testing and evaluation (ST&E) from automated vulnerability scanning and penetration testing. The purpose of system security testing is to test the effectiveness of the security controls of a system as they have been applied in an operational environment. In contrast, the potential vulnerabilities identified by automated scanning may not represent real vulnerabilities in the context of the system environment. Similarly, penetration testing is used to test the system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) provides guidance in section 2.1. The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases the control enhancements are used in an information system requiring greater protection, due to the potential impact of loss or when organizations seek additions to a basic control's functionality, based on the results of a risk assessment. Control enhancements are numbered sequentially within each control, so the enhancements can be easily identified when selected to supplement the basic control.

The ECRO does not have a contingency plan. All regional offices rely on Headquarters for contingency planning and disaster recovery. The FTC DRP and Continuity of Government kit do not address IT recovery of regional offices.

The effect is that the East Central Regional Office may take longer to recover from an incident. This is even more critical since the East Central Regional Office is the designated backup site for the FTC Data Center in Washington, DC, in the event of failure of the data centers located at the Pennsylvania Avenue and New Jersey Avenue buildings.

Recommendation

1. ASO develop a COOP plan for the Regional Offices or include the Regional Offices in the agency COOP plan to address a range of disaster scenarios up to and including destruction of the Regional Office.

2. ITM modify the DRP to address IT incidents at the regional offices in more detail. A number of recovery scenarios could be developed ranging from server and electrical failures, to fire or water release, in the Data Center extending to complete destruction of the office.

ITM/ASO Response

1. ASO accepts the finding and will develop a COOP plan for Regional Offices and/or include Regional Offices in the agency's COOP plan.

2. ITM accepts the finding and will modify the DRP to address IT incidents at the Regional Offices in more detail.

OIG Response

OIG concurs with ASO and ITM. The finding will be evaluated for compliance during the FY2007 FISMA review.

6.5 The ECRO as an alternate site for Washington, D.C. data centers

Finding #4: The East Central Regional Office does not have the resources to function as a backup site for the FTC main data center.

The East Central Regional Office has been designated as an alternate site for the FTC's Washington, DC, data centers. Based upon an interview with the director of the Regional Office and site surveys, the OIG has determined that the facility has insufficient resources to function as an alternate site.

NIST SP 800-34, Contingency Planning for Information Technology Systems, dated June 2002, states that recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the Business Impact Analysis (BIA). Several alternatives should be

considered when developing the strategy including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. Specific recovery methods further described in section 3.4.2 should be considered and may include commercial contracts with cold, warm, or hot site vendors; mobile sites; mirrored sites; reciprocal agreements with internal or external organizations; and SLAs with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS), and mirrored systems should be considered when developing a system recovery strategy.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) states that organizations should employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

FTC continues to work at developing a sound disaster recovery and contingency plan. The review of the East Central region's security and emergency response documentation identified a collection of documents that identify useful personnel safety and physical security response information. These documents include:

1. Federal Trade Commission East Central Region Cleveland Roster: This roster contains a list of East Central Regional Office staff members and their positions. The form will be used to determine if the system ACL is accurate.

2. Tenant User's Manual Eaton Center Building: This document contains emergency contact information and instructions on how to respond to a variety of emergency scenarios including fire/explosion, civil disturbance, bomb threats, building power failure, medical emergencies, natural disasters, and environmental emergencies. The document also addresses elevator usage during emergencies, fire-drill procedures, emergency communications, reporting security incidents, and evacuation procedures for disabled persons.

3. CBRE Tenant Information Form: This form contains tenant information that would be useful in an emergency. This information includes tenant name, number of employees, contact information, and daily point of contact information. This form is considered confidential by the building management company and is used for emergency purposes only.

4. Eaton Center Fact Sheet: This form provides general information about the building and suite. Information includes building name, address, technical data, and relevant contact information.

5. Occupant Emergency Plan (Abbreviated Form), GSA Form 3415 (2-80): This abbreviated form contains East Central Regional Office emergency personnel contact information. It also contains emergency procedures for fire and smoke, earthquake, severe weather, bomb threat, and civil disturbance.

A number of weaknesses were identified in connection with the plan to use the ECRO as an alternative site for Washington, DC Data Centers. Based upon interviews and site surveys, OIG determined that the facility has insufficient resources to function as an alternate site. The suite does not have sufficient space, power, or HVAC capability to handle the extra equipment required if the main data centers were disabled. Additionally, Administrative Services reported that there are no MOUs, SLAs, or agreements with GSA in place to provide these extra resources. Finally, the FTC DRP and Continuity of Government Kit do not address recovery from a disaster that takes place at a regional office.

The effect is that it may take longer to restore FTC IT operations because the East Central Regional Office would have to undergo extensive modifications to handle the additional equipment, as well as power and HVAC requirements.

Recommendations

ITM should:

1. Evaluate the cost-effectiveness of setting up backup servers at a site operated by a vendor who specializes in disaster recovery. OIG is aware that this option is not problem-free. OIT would have to establish MOUs with the vendor that would address topics that include, but are not limited to:
   - Data protection
   - Vulnerability scanning
   - Patch management
   - Response time requirement.
2. Continue to develop a permanent alternate site solution.
3. Establish MOUs and SLAs to ensure that required resources are identified and available if needed.

ITM Response

ITM accepts the finding and has had in its work plan the development of an adequate ‘warm’ backup site that would house servers and software to be used in the event of an extended, catastrophic failure at the Commission’s Headquarters. The ITM plan is to complete these arrangements with another federal agency during FY2007.

OIG Response

OIG concurs with ITM. This finding will be reviewed for compliance during the FY2007 FISMA review.

7 OMB Reporting Summary

OIG completed and submitted Section B of the FISMA submission to OMB. Generally, OIG and ITM agree on the inventory and other findings in this section.

Finding # 5: ITM's inventory is not complete.
Finding # 6: ITM is not using National Security Agency (NSA) or NIST configuration checklists.

Our review identified four systems that were not on FTCs inventory, (1) Internet Lab, (2) Redress, (3) Litigation Support Lab, and (4) Blackberry wireless system. This occurred because ITM did not follow new reporting requirements listed in OMB M-06-20. As a result, ITM's inventory is not accurate, and FTC's systems may not be in compliance with NIST or NSA configuration settings.

OMB M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, dated July 17, 2006 (M-06-20), requests that IGs provide a list of any systems they have found missing from the agency's inventory of major information systems. Agencies are required under the E-Government Act of 2002 to provide an inventory of major information systems (Pub. L. No. 107-347, §305(c)(2), codified at 44 U.S.C. § 3505(c)).

As part of this fiscal year's FISMA review, OIG was required to analyze and report on FTC's inventory, configuration management, self-assessments, POA&M process, as well as incident response and security awareness training.

M-06-20 also states that security configuration checklists are now available for computer software widely used within the federal government. The checklists may be found on the NIST Computer Security Division Web site, as well as the NSA System and Network Attack Center Web site. OMB expects agencies to use the published configurations or be prepared to justify why they are not doing so. IGs should review such use.

Finally, FISMA is unambiguous regarding the extent to which NIST C&A and annual IT security self-assessments apply. To the extent that contractor, state, or grantee systems process, store, or house federal government information (for which the agency continues to be responsible for maintaining control), their security controls must be assessed against the same NIST criteria and standards as if they were a government-owned or operated system. The accreditation boundary for these systems must be carefully mapped to ensure that federal information: (a) is adequately protected; (b) is segregated from the contractor, state, or grantee corporate infrastructure; and (c) there is an interconnection security agreement in place to address connections from the contractor, state, or grantee system containing the agency information to systems external to the accreditation boundary.

As reported above, these systems were not on the inventory: (1) Internet Lab, (2) Redress, (3) Litigation Support Lab, and (4) the Blackberry wireless system. ITM reported that Redress, Litigation Support Lab, and the Blackberry wireless system are included under the Infrastructure general support system (GSS) and that Internet Lab was under the management and control of Bureau of Consumer Protection (BCP). OIG noted that they are not listed in the current

Infrastructure C&A package. ITM confirmed this and stated that the Litigation Support Lab and Blackberry systems will be listed in the new Infrastructure C&A package which has a planned completion date of October 2006. When the new version of Redress is complete, it will be reclassified as a major application and will be listed on the inventory, certified and accredited. ITM reported that it does not include the Internet Lab because it is under the management of the BCP, and ITM has no control over it. When the new version of Redress goes into production, OIG will confirm that Redress is certified and accredited. When the Infrastructure GSS is recertified and reaccredited, OIG will confirm that the Litigation Support Lab and the Blackberry system are included in the new C&A package.

OIG determined that with the exception of Windows XP Professional, ITM has configuration management guides for the software it runs at FTC. Internet Lab workstations use the XP Professional software. This system is beyond the control of ITM. OIG also noted that the checklists used by FTC are not checklists developed by NIST or NSA. OIG also agrees with ITM that the FTC has a documented incident response policy and that security awareness training addresses the use of peer-to-peer software on FTC IT assets.

Because FTC's systems may not be in compliance with NIST or NSA configuration settings, these systems could be vulnerable to IT attacks.

Recommendations

ITM:

1. Go forward with plans to address the inventory issue.
2. Either conform to NIST or NSA configuration or document the reason for not using NIST and/or NSA configuration settings.

ITM Response

1. ITM accepts the finding that the systems (Redress, Blackberry, and Litigation Support Lab) are not listed in the inventory of minor applications.

2. ITM accepts the finding regarding the NIST/RSA configuration guidelines and will determine and document if the guidelines can be used with the FTCs current application inventory.

OIG Response

OIG concurs with ITM. This finding will be reviewed for compliance during the FY2007 FISMA review.

8 Self-Assessment Review

As part of this year's FISMA review, OIG reviewed FTC's self-assessments for its major applications and GSS. The review was designed to determine if the self-assessments are being completed annually and if they are being completed in accordance with SP 800-26 guidance.

NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, dated November 2001, identifies a framework for measuring an agency's level of compliance. The framework comprises five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement. Coupled with the NIST-prepared self-assessment questionnaire, the framework provides a vehicle for consistent and effective measurement of the security status for a given asset. The security status is measured by determining if specific security controls are documented; implemented; tested and reviewed; and incorporated into a cyclical review/improvement program, as well as whether unacceptable risks are identified and mitigated. The NIST questionnaire provides specific questions that identify the control criteria against which agency policies, procedures, and security controls can be compared. Appendix A contains a sample of the upcoming NIST SP.

OMB M-6-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006 states that FISMA is unambiguous regarding the extent to which NIST C&A and annual IT security self-assessments apply. To the extent that contractor, state, or grantee systems process, store, or house Federal government information (for which the agency continues to be responsible for maintaining control), their security controls must be assessed against the same NIST criteria and standards as if they were a government-owned or operated system. The accreditation boundary for these systems must be carefully mapped to ensure that federal information: (a) is adequately protected; (b) is segregated from the contractor, state, or grantee corporate infrastructure; and (c) there is an interconnection security agreement in place to address connections from the contractor, state, or grantee system containing the agency information to systems external to the accreditation boundary.

M-6-20 goes on to state that to meet the requirement for conducting a NIST SP 800-26 review, agencies can:

1. Continue to use NIST SP 800-26.
2. Conduct a self-assessment against the controls found in NIST SP 800-53.

Review of the self-assessments confirmed that self-assessments were conducted for:

- Infrastructure Self-Assessment ((6/20/2006)
- Hart Scott Rodino Electronic Filing System (e-Premerger) (August 1, 2006)
- Consumer Information System (CIS) Security Control Assessment (6/21/2005)
- CommentWorks^{SM} (9/14/2006)
- Documentum (9/13/05)
- Matters Management System Self Assessment (MMS) (10/17/2005)

According to ITM, Do Not Call and CommentWorks^{SM} were certified and accredited this year and therefore do not require a self-assessment however a self-assessment was prepared for CommentWorks^{SM} as part of the C&A effort. Although, a self-assessment was not developed for CIS this year, it did undergo a Security Control Assessment. The C&A for CIS expires on September 29, 2006 and should undergo a new certification and accreditation. Finally, FFS/FPPS is owned and operated by the Department of Interior (DOI) and the FTC is not responsible for its self-assessments and C&As.

It should be noted that the Internet Lab and the Litigation Support Labs are under the control of the Bureau of Consumer Protection (BCP) and beyond the control of ITM. A Security Control Assessment, risk assessment, and system security plan were developed for Internet Lab. Litigation Support Lab has undergone a risk assessment, security plan and security assessment review. However neither of these systems has been certified and accredited. This may be beyond ITM's control.

Recommendation

None

9 POA&M Management

Our review of the POA&M confirmed that ITM is completing and using the POA&M in accordance with NIST guidance. The review looked at three aspects of the POA&M process. First, the effectiveness of corrective actions to address weaknesses was reviewed and evaluated. Second, FTC's quarterly reporting to OMB was reviewed to determine if FTC is accurately reporting POA&M statistics to OMB. Finally, FTC's master POA&M sheet was reviewed to determine if it was being completed in accordance with OMB M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

OMB M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006, states that the purpose of a POA&M is to identify and track in one location an agency's security weaknesses. A POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. M-06-20 also states that agencies shall confirm the security program of the major component which operates the field offices is: (i) effectively overseeing and measuring field performance; (ii) including any weaknesses in the agency wide POA&M, and; (iii) developing, implementing, and maintaining system-level POA&Ms.

OMB M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, dated August 23, 2004, states that agencies must provide on a quarterly basis summary information on the POA&M progress and an update on IT security performance measures. OMB M-06-20 states that quarterly updates are now due to OMB on September 1, December 1, March 1, and June 1. The dates have been adjusted to accommodate the timing of agency quarterly President's Management Agenda scorecards.

Corrective Action Review

OIG reviewed the corrective action taken to correct weaknesses for the period ranging from the 4th quarter of FY 2005 through the 3rd quarter of FY 2006. For the 4th quarter FY 2005 POA&M reporting period, ITM reported that they were able to correct 16 weaknesses identified on the POA&M. OIG was able to confirm completion of 15 of those weaknesses. For the 1st quarter FY 2006 POA&M reporting period, ITM reported the correction of eight weaknesses. OIG confirmed that corrective action was taken for seven weaknesses. For the 2nd quarter FY 2006 POA&M reporting period, ITM reported the correction of 16 weaknesses. OIG confirmed that corrective action was taken for all 16 items. For the 3rd quarter 2006 POA&M reporting period, ITM completed corrective action on three program level weaknesses and one system

level weakness. OIG agrees with ITM that all the corrective actions taken for the identified POA&M items effectively address the identified weakness. Overall, OIG feels that ITM is effectively addressing weaknesses identified in various security reviews. In some instances where OIG does not agree with ITM on the completion of a corrective action, additional validation material could allow OIG to make the confirmation. Details regarding OIG's review of corrective actions can be found in Appendix B of the Independent Evaluation.

Quarterly Reporting

OIG reviewed the official quarterly OMB POA&M submissions for the FTC. The documents were used to verify the statistics FTC provided to OMB in the quarterly reports for the 4th quarter 2005 and the 1st, 2nd, and 3rd quarters of 2006. OIG confirmed that the quarterly submissions were accurate. The table below presents FTC's quarterly submissions. No further action is required.

	Total number of weaknesses identified at the start of the quarter	Weaknesses for which corrective action was completed by the end of the quarter	Weaknesses for which corrective action on track to be completed as originally scheduled	Weaknesses for which corrective action has been delayed	New weaknesses discovered following the last POA&M update
4th Qtr FY 2005					
Program-level	17	4	3	10	0
System-level	39	12	9	18	0
1st Qtr FY 2006					
Program-level	13	2	16	9	14
System-level	27	6	47	22	48
2nd Qtr FY 2006					
Program-level	25	1	16	8	0
System-level	69	15	43	13	2
3rd Qtr FY 2006					
Program-level	24	3	15	6	0
System-level	56	2	42	12	0

Review of the POA&M confirmed that ITM is completing and using the POA&M in accordance with NIST guidance.

Recommendation

None

10 Remote Access

OIG reviewed FTC's remote access policies, procedures, and controls for protecting FTC assets from unauthorized remote access attacks. The review found that FTC relies on a number of safeguards to protect its data and IT assets from unauthorized remote access. First, FTC has a documented remote access policy. FTC uses RSA SecurID tokens, user ids, and passwords for authentication. Unused tokens are kept in a secure area, and the tokens are collected when an employee no longer requires remote access or leaves the organization. Users must have their remote access request form signed by their supervisor and contractors must have their request form signed by their contract officer. FTC also has a password policy (ITM-2004-03) that provides guidance on creating strong passwords. The remote access mechanism allows five invalid login attempts before it locks the account. The account must then be unlocked by the system administrator. A warning banner appears upon login.

Testing confirmed that application forms are completed by personnel requesting remote access capability and that these forms are signed by their supervisors. RSA SecurID tokens are used for remote authentication, and unused tokens are kept in a secure area. Personnel receive training when they receive their SecurID token.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005, states that the organization should document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials should authorize each remote access method for the information system and authorize only the necessary users for each access method. The organization should employ automated mechanisms to facilitate the monitoring and control of remote access methods. The organization should use encryption to protect the confidentiality of remote access sessions. The organization should control all remote accesses through a managed access control point.

SP 800-53 goes on to say that remote access controls are applicable to information systems other than public Web servers or systems specifically designed for public access. The organization should restrict access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protect against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). The organization should permit remote access for privileged functions only for compelling operational needs. NIST SP 800-63 provides guidance on remote electronic authentication.

FTC's remote access policies, procedures, and controls for protecting FTC assets are in compliance with published guidelines.

Recommendation

None

11 Share Drive Review

OIG confirmed that there are documented policies and procedures that address maintenance, media protection, and incident response. In addition, there are a variety of policies and

procedures, and technical controls that control what files users can access. There is a documented list of authorized maintenance personnel.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005, states that account management include the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization should identify authorized users of the information system and specifies access rights/privileges. The organization should grant access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization should require proper identification for requests to establish information system accounts and approve all such requests. The organization should specifically authorize and monitor the use of guest/anonymous accounts and remove, disable, or otherwise secure unnecessary accounts. The organization should ensure that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers should be notified when users' information system usage or need-to-know changes.

Tests conducted in conjunction with this report confirmed that ACLs are up to date and personnel are limited to only those drives they need to do their jobs. The IDS is running and will automatically alert appropriate personnel if certain thresholds for specific events are met.

Recommendation

None

12 Private Automatic Branch Exchange (PBX)/Voice Over Internet Protocol (VOIP) Review

OIGs review of the PBX/VOIP confirmed that there are controls in the areas of system and services acquisition; certification, accreditation, and security assessments; configuration management; maintenance; system and information integrity; and system and communications protection as they relate to the PBX/VOIP.

Also, there are physical security controls in place to protect the servers where the PBX/VOIP is located. The Data Center and phone closets are locked at all times. The Data Center requires card key access and is monitored by surveillance cameras. The phone system is also included under the FTC Infrastructure C&A. The servers were built and maintained according to vendor best practices and FTC configuration management policy. Additionally, unneeded services on the servers and software are disabled, default administrative passwords are changed, and FTC maintenance policy and procedures are followed.

The system is protected by a firewall, and only calls within FTC controlled space are transmitted via VOIP. An ACL is also used to control access to the servers. Once a long distance call travels outside of FTC controlled space, it is transmitted over Public Switch Telephone Network (PSTN).

PBX

The phone system resides on four Cisco MSC35 servers running a Cisco customized version of Windows 2000, Cisco Call Manager v 3.3.3. Maintenance terminals are located in restricted areas. Maintenance features are turned-off when not needed. Passwords follow FTC password policy. There are also controls in place to protect against voice mail hacking.

Voice-Over Internet Protocol (VOIP)

VOIP uses Cisco proprietary software and is protected via firewall. Encryption is not used or required. Voice and data are on separate, logically different networks. VOIP is not allowed where the gateway interfaces with the PSTN.
Remote access to the VOIP servers is restricted to the virtual private network (VPN), requires SecurID tokens, and is limited to personnel responsible for the system. The servers are clustered and are connected to backup power generators and UPS.

NIST SP 800-58, Security Considerations for Voice-Over IP Systems, January 2005, states that agencies should be aware that physical controls are especially important in a VOIP environment and deploy them accordingly. The guidelines also state that the organization must examine and acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VOIP systems. VOIP ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VOIP systems.

Recommendation

None

13 Government Equipment Usage Procedures

OIG reviewed FTC's process for processing hard drives for systems that were either excessed or surplused. The review was conducted using interviews, site surveys, document review, and observation. The results of the review follow.

Finding # 7: Government equipment usage procedures do not track hard drives.

Hard drives are neither being inventoried nor tracked. The reason hard drives are not tracked after being removed from devices is because it has never been identified as a requirement. Additionally, FTC inventory generally tracks the central processing unit (CPU), but not the components of the CPU. As a result of not tracking hard drives, with respect to what devices they came from and in what boxes the drives are stored, it is difficult to track down hard drives for an investigation.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) states that organizations should:

1. Develop, disseminate, and periodically review/update: (i) a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, and

compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.

2. Affix external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The guidance allows organizations to exempt agency-specified types of media or hardware components from labeling so long as they remain within a secure environment.

3. Physically control and securely store information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.

4. Control information system media (paper and electronic) and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

5. Sanitize information system digital media using approved equipment, techniques, and procedures.

6. Track, document, and verify media sanitization actions and periodically test sanitization equipment/procedures to ensure correct performance.

7. Sanitize or destroy information system digital media before its disposal or release for reuse outside the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.

ITM's Tech Center is responsible for managing hard drives. ITM has taken steps to ensure that data is removed from hard drives on computers. There are documented procedures for processing surplus and excess equipment. Basically, hard drives from excessed computers are removed from devices when the computers are decommissioned. The drives are placed in a locked metal storage container. The containers are stored in a secure area that requires card key access to both the computer maintenance center and the room in the computer maintenance center where the containers are stored. When the metal storage containers are full, the drives are packed into cardboard boxes and stored until they are picked up by Capitol Shredding and destroyed.

Equipment targeted for reuse is kept intact for two weeks and stored in the FTC warehouse. During this two week period, the previous user can request access to the data on the drive. After that two-week period, the drives are re-imaged and reassigned.

Hard drive removal and destruction procedures are documented. This documentation provides instructions on how to complete the SF-120 forms and how to prepare hard drives from excessed machines for destruction. The instructions state that hard drives that meet or exceed a minimum size are reformatted and placed in the parts room for later use; while, smaller drives should be removed. The instructions state that personal computers that are delivered to customers must be re-imaged.

Hard drives from excessed devices are not tracked once they are removed from the computer.

Recommendation

ITM needs to begin tracking hard drives after they are removed from devices. This could be achieved by adding one or two more entry fields on the appropriate forms to identify the serial numbers of the CPU and the hard drive.

ITM Response

ITM accepts the finding and will implement a process to track hard drives that are removed from devices.

OIG Response

OIG concurs with ITM. This finding will be evaluated for compliance during the FY2007 FISMA review.

14 CommentWorks[SM]

FTC has contracted with ICF Consulting (ICF) for the use of Commentworks[SM] software to receive and process comments from the public on proposed regulatory action. CommentWorks[SM] was identified as one of the systems to be evaluated for this year's FISMA review. The evaluation consisted of a review of the CommentWorksS[M] C&A package and an interview with the CommentWorks[SM] FTC program manager and a representative from ICF, the contracting company that owns and operates CommentWorks[SM] for FTC. The review identified two findings that are discussed below.

Finding # 8: The CommentWorksSM C&A package does not conform to NIST guidance.

The CommentWorks[SM] security plan does not address all topic areas identified in NIST SP 800-53. This occurred because of ICF's lack of familiarity with NIST and OMB guidance. As a result, FTC may not be aware of the risks associated with running CommentWorks[SM] in the production environment.

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, was developed by NIST in furtherance of its statutory responsibilities under the FISMA of 2002, Public Law 107-347. Specifically, FISMA tasked NIST with the responsibility for developing standards and guidelines, including developing standards for categorizing information and information systems.

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability. FIPS PUB 199 defines three levels of potential impact (high, moderate, or low) on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

These standards shall apply to all information within the federal government other than classified information and national security systems. Agency officials shall use the security categorizations described in FIPS PUB 199 whenever there is a federal requirement to provide such a categorization of information or information systems.

NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, dated February 2006, requires the use of NIST SP 800-53 security controls. Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain (i) the security control title; (ii) how the security control is being implemented or is planned to be implemented; (iii) any scoping guidance that has been applied and what type of consideration; and (iv) whether the security control is a common control and who is responsible for its implementation.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated July 2002, differentiates ST&E from automated vulnerability scanning and penetration testing. The purpose of system security testing is to test the effectiveness of the security controls of a system as they have been applied in an operational environment. In contrast, the potential vulnerabilities identified by automated scanning may not represent real vulnerabilities in the context of the system environment. Similarly, penetration testing is used to test the system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) provides guidance in section 2.1. The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases the control enhancements are used in an information system requiring greater protection, due to the potential impact of loss or when organizations seek additions to a basic control's functionality, based on the results of a risk assessment. Control enhancements are numbered sequentially within each control, so the enhancements can be easily identified when selected to supplement the basic control.

CommentWorks^{SM} is ICF Consulting's e-Government Web-based public participation system. With this system, government agencies and their consultants efficiently manage public comments on controversial initiatives. The public can submit and view comments and other materials through the Web. CommentWorks^{SM} software is a Web-enabled application that streamlines the process of tracking and compiling public comments. Features include the following:

1. Supports public entry of comments into the database through a public Internet form that supports multiple choice questions, free-form text comments, and file attachments.

2. Allows project staff real-time access to the full text of public comments and relevant comment tracking and identification data (e.g., comment number, commenter name, commenter organization type, date received, etc.) through a password-protected and encrypted Internet site.

3. Allows batch importation of text-based electronic comments compiled from sources other than the Internet form.

4. Allows the assignment of unique user privileges to members of the comment team with the appropriate privileges to create, view, edit and/or approve comment letters, summaries, and responses, and to track the progress of comment processing.

5. Includes a message area where members of the comment team can post messages by issue or team member.

6. Provides a multi-tiered outline of issue categories related to the initiative by which public comments and/or selected excerpts from public comments are to be categorized. The outline can be modified at any time during the comment analysis process by adding, deleting, or reorganizing categories at any level.

7. Enables the identification and selection of salient excerpts within the comment letter text and association of these excerpts with one or more issues on the outline. If the outline is modified, the system automatically renumbers the affected issue categories and maintains links between these categories and the associated excerpts, summaries, and responses.

8. Allows viewing and reporting of comment excerpts, summaries, and responses by one or more issue categories.

9. Allows reports and comment data to be exported to common word-processing or spreadsheet file formats for refinement, editing, and archiving.

10. Fully functional and has been demonstrated on over 20 projects and, therefore, requires no further software development.

11. Fully scaleable from one to any number of initiatives on which public comments are to be received.

12. Provides developed and tested user training and support materials.

The FTC Public Comment Form is located at the ICF headquarters data center. The data center is controlled and maintained by the ICF Computer Information Technology (CIT) Group. The data center contains industry standard requirements (UPS, access floor systems, building grounding

and lightning protection systems, fire protection systems, access key cards, cipher lock controls) to adequately house and host Sensitive but Unclassified data.

Sensitivity/criticality for CommentWorks[SM] was described in the following way:

Confidentiality – Most of the information managed through CommentWorks[SM] becomes public (e.g., posted on the Internet) soon after it is received because it is part of the public and administrative record. The public comment form may or may not, at FTC's discretion, contain limited personal information from the commenters including name, address, phone number, and/or e-mail address. FTC also decides which, if any, of this information is required–in most circumstances comments are completely anonymous. Though not asked to do so, public commenters occasionally include personal identifying information in the body of their comment, and often this information is redacted before the comment is made public. In every instance, the public comment form includes a privacy statement indicating how FTC intends to use the information it receives through the form. The form does not solicit information on email, phone number, social security number (SSN), or any financial information. No confidential business information is required. Instructions specifically alert users that all information is publicly available on the Web.

Integrity – The substance of the comments on the forms must be maintained to ensure compliance with the Administrations Procedure Act (APA) and with federal records management requirements and generally to ensure that the views expressed in the comments are accurately conveyed to FTC staff.

Availability – The public comment form component of the system must be available for the specific public comment periods defined for each initiative (in most cases, 30 days). Other delivery methods are available to the public to submit their comments (i.e., the FTC Web-based form is not the only means to submit comments). Paper comments may also be submitted via mail, courier, or overnight delivery. The comment analysis components of the system must generally be available during normal working hours of FTC staff.

The sensitivity/criticality of the system is not determined in accordance with FIPS Pub 199.

The CommentWorks[SM] security plan doe not address all topic areas identified in NIST SP 800-53. In areas addressed, the detail required by SP 800-53 was not provided. Topics not covered were C&A, physical/environmental, system and information integrity, identification, system communication protection. Additionally, the security plan was not completed in accordance with NIST SP 800-18.

Recommendations

ITM:

1. Develop a CommentWorks[SM] security plan in accordance with FIPS Pub 199, NIST SP 800-18, and NIST SP 800-53.
2. ICF develop a contingency plan in order to maintain CommentWorks[SM] operations.

ITM Response

ITM accepts recommendations 1 and 2 and will require CommentWorks[SM] to update the SSP to conform to the format of NIST SP 800-18 and SP 800-53 during FY07. ITM will require CommentWorks[SM] to develop a contingency plan during FY 07.

OIG Response

OIG concurs with ITM. This finding will be evaluated for compliance during next year's FISMA review.

Finding # 9: FTC managers responsible for CommentWorksSM are not notified when FTC personnel leave the organization or are transferred within the organization and no longer need access to the system.

NIST SP 800-53 *Annex 1, Minimum Security controls for Moderate Baseline* (systems), requires that organization manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes (SP 800-53 Annex 1, p 34).

At this time, the FTC managers responsible for CommentWorks[SM] are not notified when personnel no longer need access to CommentWorks[SM]. This could lead to unneeded accounts being left active longer than they need to be. These unused accounts could be used by hackers to gain access to the system.

Recommendation

Modify FTC personnel procedures so that FTC managers responsible for CommentWorks[SM] are notified when employees no longer require access to the system.

ITM Response:

ITM accepts this finding and will add the System Owner of CommentWorks[SM] to the existing monthly report of active users. This report provides the System Owner of the application with a

listing of all FTC employees with access to their system to allow the System Owner to remove the access of individuals who no longer require it.

OIG Response

OIG concurs with ITM. This finding will be evaluated for compliance during the FY2007 FISMA review.

15 Internet Lab Review

The Internet Lab was the second system evaluated during the FISMA review. The Lab is comprised of stand alone computers that are not connected to the FTC IT Infrastructure and are not traceable to the agency. They are used in connection with investigations of consumer fraud by the Bureau of Consumer Protection (BCP). The review consisted of an interview with BCP personnel responsible for the system, a review of Internet Lab risk assessment and security plan, and a site survey of the labs at Headquarters and at the New Jersey Avenue office. Two findings were identified.

Finding # 10: Physical security controls for Internet Lab need improvement.

For physical security SP 800-53 states that the organization should develop, disseminate, and periodically review/update: (i) a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

In the area of maintenance, NIST SP 800-53 states that the organization should develop, disseminate, and periodically review/update: (i) a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. The organization should also schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

The labs are located in secure facilities that are controlled by the FTC. There are guard desks at the entrances. Each lab requires card key access. Sprinkler systems are installed in each room. The New Jersey Avenue lab does not have windows, and the Pennsylvania Avenue lab has blast proof windows. However, a number of vulnerabilities were identified:

Room H283, 600 Pennsylvania Avenue

- No fire extinguishers are located in the lab.
- There is no secondary air conditioning system in the lab.
- There is no contingency plan for the Internet Lab.
- There is the potential that data could be transferred from the Internet Lab and loaded onto the Infrastructure GSS.

Room 3238, 601 New Jersey Avenue

- Room 3238 does not have true floor to ceiling walls (Site Survey). There is a three foot space between the top of the wall and the true ceiling.
- There is no secondary air conditioning system in the lab.

The reason for some of these findings is that the Internet Lab is a relatively small system of low sensitivity/criticality that has been independent of ITM.

Recommendation(s)

1. Evaluate the possibility of placing Internet Lab servers in the Data Center. ITM should determine if this move is feasible, practical, cost-effective, and useful. Internet Lab should still function as a standalone system.

2. Continue efforts to include the Internet Lab under the Infrastructure GSS. The Infrastructure C&A package should be updated to reflect these changes.

BCP Response

1. Placing the Internet Lab servers in the Data Center would provide additional physical security. Until the new data facility is placed in operation, there are power and cooling limitations that preclude taking this action. The projected completion date is summer of 2007.

2. The Division of Planning and Information (DPI), in conjunction with the CISO, will undertake this analysis and present the conclusions to the IG in the coming year.

OIG Response

OIG concurs with BCP's response. BCP should coordinate with ITM to reach an acceptable solution. OIG will evaluate for compliance during the FY2007 FISMA review.

Finding # 11: Policies, procedures, and related security documentation for the Internet Lab either do not exist or are not documented.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) identifies controls for the following areas:

Organizations should develop, disseminate, and periodically review/update: (i) a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

In the area of personnel security, SP 800-53 states that the organization should assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The organization should review and revise position risk designations on a scheduled basis. The organization should also screen individuals requiring access to organizational information and information systems before authorizing access.

When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.

Finally, in the area of system and information integrity, SP 800-53 states that the organization should develop, disseminate, and periodically review/update: (i) a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

A number of safeguards were identified that are used to protect the Internet Lab and its data. These controls include card key access to the Internet Lab, archiving data, tracking loaned laptops, conducting hardware and software inventories, and fire and smoke detection and extinguishers. However, the following vulnerabilities were also identified:

- Check-in, Check-out Move notifications are not sent to Internet Lab managers when agency employees are transferred or leave the FTC.
- There are no documented policies, procedures, or forms for requesting, approving, or creating/removing user accounts for the Internet Lab. OIG was also advised that user IDs and passwords are not required for users to log onto and access Internet Lab workstations.
- There is no contingency plan for the Internet Lab. In the event of a catastrophic event that would render either the Pennsylvania Avenue or New Jersey Avenue labs unusable, the remaining lab would be used as the alternate site.
- There are no documented maintenance procedures.
- There are no documented backup procedures. Backups are not conducted at this time; however, raw data is archived.
- There is no configuration management build documentation to provide guidance on how to build servers and workstations.
- Internet Lab systems are not scanned to check for vulnerabilities.
- There are no documented procedures for reporting system flaws.

The cause for these problems is that the Internet Lab is controlled by the BCP, which functions independently of ITM and, therefore, does not fall under the under the authority of ITM's policies and procedures.

The effect of this is that the Internet Lab does not have many of the controls in place that protect other FTC IT assets. Therefore, the Internet Lab may not be as secure as other FTC systems. Also, the effect of not requiring users to logon to the Internet Lab workstation is that there is no way to track user activity. A user could potentially engage in improper activity using FTC assets without fear of discovery.

Recommendations

BCP:

1. Include Internet Lab under ITM's operational and technical management or BCP adopts and implements ITM's IT policies, procedures, and configuration management plans. The Internet Lab's C&A package should be modified accordingly.

2. ITM and BCP should evaluate moving Internet Lab servers to the FTC Data Center, so the application can benefit from the Data Center's existing physical security and contingency safeguards. OIG notes that the Internet Lab is considered a low sensitivity/criticality and realizes that this recommendation may be determined to be impractical or not cost-effective.

3. Modify Check-in, Check-out Move procedures so that personnel responsible for the Internet Lab are notified of personnel changes that affect Internet Lab access. User accounts should be immediately disabled and then removed at a later date.

4. Document policies, procedures, and forms for requesting, reviewing/approving, and creating/removing user accounts.

5. Develop a contingency plan for the Internet Lab.

6. Conduct vulnerability assessment scans on Internet Lab servers and workstations in accordance with ITM policy.

7. Document backup and restore procedures.

8. Require user IDs and passwords for accessing Internet Lab workstations.

9. Implement logging to track user activity.

10. Develop and implement policies and procedures that restrict users from placing files obtained from the Internet Lab on the Infrastructure GSS. The policy and procedures should, if necessary, identify procedures for scanning, sanitizing, and quarantining files that need to be placed in the Infrastructure environment.

BCP Response

1. DPI will perform a review of ITM polices, procedures, and configuration management plans to determine which would be appropriate for the Internet Lab and then apply them with appropriate modifications to the operations of the Internet Lab. The results will be presented to the OIG at the conclusion of this review.

2. Placing the Internet Lab servers in the Data Center would provide additional physical security. Until the new data facility is placed in operation, there are power and cooling limitations that preclude taking this action. The projected completion date is summer of 2007.

3. Internet Lab access was added to the CICOM Form 426 in January, 2006. As a result, Internet Lab staff will be notified of personnel changes that affect Internet Lab access.

4. The policies for user access to the Internet Labs will be documented.

5. The current Lab plan, which asks users to move between Labs if problems arise in one, is sufficient for all but catastrophic situations. While very important to BCP, the work of the Bureau could continue while the Labs were rebuilt either in place or at an alternative location in the event of a large-scale failure. As a result, no contingency plan is required since the facility is not mission-critical.

6. Periodic assessment scans will be performed by Bureau staff, and an independent scan will be performed at least annually. Results of the assessment scans will be evaluated based upon the mission and requirements of the Internet Lab.

7. Only spam data meets the threshold to be backed up. The data is archived on an ongoing basis. ITM will assist the Bureau in reestablishing a backup process for this data.

8. DPI believes that individual user IDs and passwords would be very burdensome and interfere with the work of the Lab. Because of the limited number of PCs and the fact that more than one person may work on a project, we cannot assign individuals to specific PCs. Therefore, multiple profiles will build up on each system. The profiles will have to be recreated each time that a user logs into a PC that has been re-imaged, which is a frequent occurrence. Data created under one user's profile will be difficult for another user on the project to find, and issues may arise when a second project member must add data to an existing evidence repository. Individual IDs and passwords also would create a significant administrative burden on a small IT group.

   We always have been aware of the need for workstation security, as evidence by the fact that we installed the first proximity reader system in an internal FTC facility. As an alternative to user IDs, we propose a sign-in system. Each workstation would have a sheet asking for name, log-on and log-off times, and project name. The sign-in process would be augmented by walk-around monitoring and periodic cross-checking against the proximity reader logs.

9. DPI accepts the need to identify inappropriate use of Lab PCs. Internet Lab staff have made a practice of checking PC use by observing staff behavior since the Lab opened and

have found that other users are sensitive to inappropriate use and will report it to us. DPI believes that automated logging software has the potential to create problems in the evidence gathering process and, contrary to standard Lab practice, will introduce programs that are not part of a typical home PC setup.

10. DPI understands the potential for infecting FTC systems with files gathered in the Lab, and will post alerts on all Lab PCs that files downloaded in the course of investigations should be scanned before transferring them to desktops or laptops used on the production network.

OIG Response

OIG concurs with DPI's response to recommendations 1 thorough 7, 9 and 10, and suggests that DPI work with ITM to determine what modifications would be appropriate to the operations of the Internet Lab. These findings will be evaluated for compliance during FY2007 FISMA review.

OIG does not concur with DPI's response to recommendation 8. The anonymous use of computers in the internet lab in the past has provided an opportunity for computer misuse. We do not agree that the relatively insignificant burden associated with this recommendation outweighs the need for effective controls to protect the agency from the potential for humiliation arising from misuse of its IT equipment. DPI should either implement this recommendation or work with ITM to implement alternative measures to effectively prevent computer misuse in the internet lab. This finding will be evaluated for compliance as part of the POAM review.

16 Disaster Recovery Plan

OIG reviewed ITM's disaster recovery efforts to evaluate the effectiveness of the plan and, if necessary, identify any potential problems that ITM may face if the plan would ever need to be activated. The review consisted of document reviews, interviews, and site surveys of the Data Center and backup sites located at 601 New Jersey Avenue and Cleveland, Ohio. The results of the review follow.

Finding # 12: FTC's Disaster Recovery Plan needs further development.

NIST SP 800-34, Contingency Planning for Information Technology Systems, dated June 2002, states that recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, the type of system, and its operational requirements. Specific recovery methods further described in

section 3.4.2 should be considered and may include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and SLAs with the equipment vendors. In addition, technologies such as RAID, automatic fail-over, UPS, and mirrored systems should be considered when developing a system recovery strategy.

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) states that organizations should employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

SP 800-53 also states that the organization should identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

The FTC is making significant progress in developing a comprehensive disaster recovery plan. FTC has also developed a Continuity of Government kit, and there are plans to have a cold site available by FY 2008.

In the short term, however, FTC faces a number of potential challenges. There are currently two backup sites. The primary site is a server room located at 601 New Jersey Avenue. The secondary site is the East Central Regional Office located in Cleveland, Ohio. As noted in section 6.5, supra., the ECRO does not have the resources to function as a backup site. The same is true at the New Jersey Avenue site. Specifically:

1. There are no moisture detectors beneath the raised floors in the data centers at headquarters and New Jersey Avenue.
2. There is insufficient space, power, and HVAC capability at both designated alternate sites.
3. Transportation plans or procedures are not identified for transporting key personnel to the East Central Regional Office.
4. The current DRP does not reference the Administrative Services Continuity of Operations Plan and Continuity of Government pack.

Review of the Central Computer Systems & PBX Disaster Recovery Plan, May 2006, found that it addressed the following areas:

Objective
Assumption
Responsibility
Off-site Storage
Scope of coverage
Event detection
Team leader responsibilities and checklist
Restoration and return to the permanent facility
Priority for restoration of application systems
Maintenance outage response
Priority for restoration of application systems

Maintenance outage response
Catastrophic disaster response

Other areas covered include:

Servers, network and storage devices
Power down/up procedures
Emergency management team contact information
Network configuration
Oracle startup/shutdown procedures
Backup procedures
Iron Mountain off-site tape pick-up and delivery
Restoration procedures
Server/Web site IP listing
Receipt of disaster recovery plan
Disaster recovery change control page

A copy of the DRP is located at the off-site tape/storage site. There are documented procedures for notification of appropriate personnel for the initiation of the DRP in the event of an incident. Steps for recovery from incidents are also discussed. The DRP identifies the roles and responsibilities of recovery team members. Systems with 24x7x4 maintenance response times are identified. The effects of a catastrophic event on various IT and telephony services are discussed. The DRP also discusses the processes that would go into effect to maintain operations. The alternate site for the 600 Pennsylvania Avenue facility is the 601 New Jersey Avenue building. The Building at 601 New Jersey Avenue has two UPS systems with a battery life of three hours.

Weaknesses found in the DRP include:

1. The alternate site, if the disaster occurs at 601 New Jersey Avenue building, is incorrect. The DRP identifies the alternate site for the 601 New Jersey Avenue building as 601 New Jersey Avenue.
2. The East Central Regional Office, located in Cleveland, Ohio is not identified as the alternate site for the Data Center.
3. The review also found that purchase procedures for purchasing replacement are not documented
4. The DRP does not include any contracts, MOUs, or ISAs that would provide information on what organizations or vendors are responsible for and response times.
5. Transportation options for getting key personnel to Cleveland are not addressed.

The source of these problems may stem from the fact that the DRP is still evolving. Additionally, ITM may be looking for a cost-effective, short-term solution for a low probability occurrence while it directs its resources to developing an effective permanent solution. Many of the weaknesses identified in the DRP could be addressed during one of its quarterly updates.

Recommendations

ITM:

1. Evaluate the feasibility of installing moisture detectors beneath the raised floor of the data centers.
2. Make arrangements with vendors to have sufficient space, power, and HVAC capability available at the designated alternate sites in the event that service from the main data center is disrupted.
3. Establish and document transport plans for key personnel who will be setting up the alternate site.
4. Ensure that the DRP references other related emergency documentation (e.g., the Continuity of Operations Plan and the Continuity of Government kit).
5. Make corrections to the DRP and include related MOUs and ISAs in the DRP.
6. Evaluate the possibility of establishing a hot site for the FTC Data Center, including the possibility of using a private vender.
7. Make corrections to the DRP:
    a. Identify alternate site for the New Jersey Avenue data center.
    b. Include purchase procedures.

ITM Response

ITM accepts the findings and will work with ASO to address the recommendation during FY2007.

OIG Response

OIG concurs with ITM's response to recommendations 1 thorough 7. OIG will evaluate for compliance during the FY2007 FISMA review.

17 Infrastructure Scan Results Summary

The OIG also conducted an internal scan of the FTC network environment on September 7 and 8, 2006. The results will be reported to the agency under a separate document.

18 Mobile Media Security

OIG is in the process of reviewing FTC's Mobile Media security efforts to determine how effectively they are conforming to OMB M-06-16 *Protection of Sensitive Agency Information.*

OMB M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006. In an effort to properly safeguard our information assets while using information technology, it is essential for all departments and agencies to know their baseline of activities.

The NIST provided a checklist for protection of remote information (see attachment). The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed, from outside the agency location. In addition to using

the NIST checklist, it is recommended that all departments and agencies take the following actions:

1. Encrypt all data on mobile computers/devices which carry agency data, unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual he/she may designate in writing.
2. Allow remote access only with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access.
3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity.
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days, or that its use is still required.

The status of FTC's laptop and mobile media protection was discussed during a series of informal meetings with the individuals listed above. At the time of the discussions, the FTC was in the process of developing a laptop policy that will identify the things users must do to protect data stored on the laptop hard drive. Currently, data protection is discussed during security awareness training, and laptops are password-protected. Additionally, The FTC issued a memo after the incident when Veteran Administration (VA) data containing personally identifiable information was stolen from a VA employee's home. The memo was to remind personnel of their responsibility to protect FTC data. ITM is also in the process of purchasing and implementing encryption software to protect data stored on FTC laptops. Finally, on September 5, 2006 the FTC Chairman issued a memorandum detailing steps to be taken to assure the security of personally identifiable information on mobile media.

OIG will wait until ITM has completed its evaluation and has developed policies and procedures to address these issues. At that time, the OIG will review the policies to evaluate their effectiveness based upon metrics identified in OMB M-06-16. The effectiveness of the agency's efforts in this area will be fully addressed in next year's FISMA Report.